North Carolina Department of Cultural Resources
Division of Archives and Records

STATE ARCHIVES
of NORTH CAROLINA

Sample Electronic Records and Imaging Policy
For Use by Local and State Agencies

June 2013

[This policy is modeled after the Department of Cultural Resources guidance *Guidelines for Managing Trustworthy Public Records Produced by Information Technology Systems*. This model policy applies to both born-digital electronic records and electronic records generated by imaging systems. Elements specific to state or local agencies are noted and should be adopted accordingly. This policy should be tailored by the party responsible for the custodianship of an agency's or department's electronic records to the agency's specific electronic records management practices wherever applicable, and provide as much detail as possible. This policy incorporates two additional forms, the *Electronic Records Self-Warranty* form and the *Request for Disposal of Original Records Duplicated by Electronic Means* form.

The North Department of Cultural Resources requires that any agency that images its records as a part of its records retention practices sign this policy after tailoring it to meet agency needs. This policy is also a requirement for agencies maintaining electronic records which have retention periods of ten or more years. When completing this policy, delete portions in brackets.]

Subject: ____________________ Policy Number: ____________________
Effective date: ____________________ Modified date: ____________________

Type of Government Office: County ( ) Municipal ( ) State Agency ( ) *Other ( )
For Other, enter name of "parent"
agency unless unassigned: ________________________________
County/Municipality/Agency: ________________________________
Name of Office: ________________________________
Office Address: ________________________________
Phone: ______________ Fax: ________________ Email: ____________________

*Includes assigned and unassigned offices (authorities, boards, bureaus, commissions, councils, private/public hybrid entities, etc.)

Table of Contents

1. Purpose

[Describe the purpose of this policy. What records does it protect, what information technology systems are used by the agency, and when will this policy be updated?]

The records covered by this policy are in the custody of **[agency name]** and are maintained for the benefit of agency use in delivering services and in documenting agency operations. This electronic records policy reflects guidelines set in the North Carolina Department of Cultural Resources publication, *North Carolina Guidelines for Managing Public Records Produced by Information Technology Systems.* Complying with this policy will increase the reliability and accuracy of records stored in information technology systems, and will ensure that they remain accessible over time. Exhibiting compliance with this policy will enhance records' admissibility and acceptance by the judicial system as being trustworthy.

All public records as defined by North Carolina G.S. § 132-1 are covered by this policy. This includes permanent and non-permanent records, and confidential and nonconfidential records. These classifications may warrant different treatments when processing the records. This policy serves as basic documentation of the procedures followed by the department in imaging, indexing, auditing, backing up, and purging electronic records in accordance with the disposition schedule, and in handling the original paper record, if applicable.

[Applicable to agencies with an imaging program] This policy also serves to protect those records digitized by the agency's **[in-house or contracted]** imaging system, which reduces required storage space for original documents as the agency transitions to a "paperless" digital system, and provides instant and simultaneous access to documents as needed.

[Applicable to local agencies] The form provided in Section 8 of this document, *Request for Disposal of Original Records Duplicated by Electronic Means*, is completed and submitted to the Department of Cultural Resources whenever this agency wishes to dispose of a new series of paper records that have been digitized.

This policy will supersede any electronic records system policy previously adopted. This policy will be reevaluated at a minimum of every **[five]** years, or upon the implementation of a new information technology system, and will be updated as required. A copy of this policy will remain on file at the Department of Cultural Resources.

2. Responsible Parties

[Describe the electronic records management responsibilities of the persons or departments responsible for adhering to this policy. Tailor this section to reflect the actual parties and their responsibilities within your agency. To go into effect,

this policy will be signed by both a records custodian who manages records creators, and an IT professional (or other project supervisor).]

- Agency Supervisor/Division Director
- IT Department
- **[For state agencies]** Chief Records Officers
- Records Creators

Agency Supervisor/Division Director
Responsibilities include:

1. **[For state agencies]** Appointing Chief Records Officers
2. Determining access rights to the system
3. Approving system as configured by IT
4. **[For agencies with an imaging program]** Performing quality assurance checks by sampling the agency's/division's imaged records before the original documents are destroyed

IT Department
Responsibilities include:

1. Installing and maintaining equipment and software
2. Configuring the system according to department needs, including creating and testing applications and indexes
3. Controlling access rights to the system
4. Maintaining documentation of system hardware and software
5. Establishing audit trails that document actions taken on records stored by the information technology system
6. Providing backups for system records, and recovering deleted imaged records when necessary
7. Completing disaster recovery backup at least once every two years
8. Establishing and providing training on equipment and software, documenting such training, and providing remedial training as needed. **[Such training includes, but is not limited to, training on the imaging system.]**
9. **[For agencies with an imaging program]** Creating and updating detailed procedural manuals describing the imaging process and equipment

[For state agencies] Chief Records Officer
Responsibilities include:

1. Coordinating all agency requests for records assistance, records or technical training, and other offered consultative services with the Government Records Section
2. Coordinating interactions between the agency business units and the Department of Cultural Resources in preparing an inclusive inventory of and schedule for records in agency custody and in establishing a time period for the retention and disposal of each records series

3. Assuring that public records are kept in safe but accessible places
4. Assisting in the timely transfer of semi current records to the State Records Center
5. In cooperation with the Department of Cultural Resources, establishing and maintaining a program for the selection and preservation of agency records considered essential to the operation of government and to the protection of the rights and interests of citizens.

Records Creators

Responsibilities include:

1. Attending and signing off on training conducted by IT staff or by the Department of Cultural Resources
2. Creating passwords for computers that are long, complex, and frequently changed
3. Creating and managing electronic records in their purview in accordance with these policies and other guidance issued by the Department of Cultural Resources, and complying with all IT security policies
4. Reviewing the system records annually and purging records in accordance with the retention schedule
5. **[For agencies with an imaging program]** Carrying out day-to-day processes associated with the agency's imaging program, including:
    - Designating records to be entered into the imaging system
    - Noting confidential information or otherwise protected records and fields
    - Removing transient records
    - Completing indexing guide form for each record being scanned
    - Reviewing images and indexing for quality assurance
    - Naming and storing the scanned images in designated folders
    - Once approved, destroying or otherwise disposing of original records in accordance with guidance issued by the Department of Cultural Resources.
    - Conducting any necessary batch conversions or batch renaming of imaged records
6. **[Applicable to public employees approved to telecommute or use mobile devices]** Public employees who have been approved to telecommute or use mobile computing devices must:

    - Comply with all information technology security policies, including the agency and statewide acceptable use policies, as well as all statutes and policies governing public records
    - Back up information stored on the mobile device daily to ensure proper recovery and restoration of data files
    - Keep the backup medium separate from the mobile computer when a mobile computer is outside a secure area

3. Availability of System and Records for Outside Inspection

[Describe how the agency complies with requests for pretrial discovery of the agency's electronic records, and how the agency intends to lay a proper foundation for the purpose of ensuring the admissibility of its records into evidence should legal proceedings arise. Also describe how the agency complies with public records requests for records maintained electronically.]

This agency recognizes that the judicial system may request pretrial discovery of the information technology system used to produce records and related materials. Agency personnel will honor requests for outside inspection of the system and testing of data by opposing parties, the court, and government representatives. Records must be available for inspection and audit by a government representative for the full period required by law and approved records retention schedules, regardless of the life expectancy of the media on which the records are stored. Records must continue to exist when litigation, government investigation, or audit is pending, imminent, or if a court order may prohibit specified records from being destroyed or otherwise rendered unavailable.

In order to lay a proper foundation for the purposes of admitting the agency's electronic records into evidence, the agency will be able to provide up-to-date, detailed documentation that describes the procedural controls employed in producing records; procedures for input control including tests used to assure accuracy and reliability; and evidence of the records' chain of custody. In addition to this policy, such documentation includes:

- Procedural manuals
- System documentation
- Training documentation
- Audit documentation
- Audit trails

The agency will also honor inspection and copy requests pursuant to N.C. G.S. § 132. The agency should produce the records in the order they were created and used in the course of business, and in the format in which they were created, unless otherwise specified by the requesting party. However, the agency should produce the records in any format it is capable of producing if asked by the requesting party. If it is necessary to separate confidential from non-confidential information in order to permit the inspection or copying of the public records, the public agency will bear the cost of such separation.

4. Maintenance of Trustworthy Electronic Records

[Describe the processes by which electronic records are produced and managed, including how a record is created, named, saved, accessed, and transferred from one storage medium to another.]

- Produced by Methods that Ensure Accuracy
- Maintained in a Secure Environment
- Associated and Linked with Appropriate Metadata
- Stored on Media that are Regularly Assessed and Refreshed

Produced by Methods that Ensure Accuracy

All platforms used by the agency to create and manage electronic records, including email clients, social media platforms, and cloud computing platforms conform with all Department of Cultural Resources' policies and all applicable security policies.

Electronic files are named in accordance with the *Best Practices for File-Naming* published by the Department of Cultural Resources. **[Define your agency's file-naming standards. What abbreviations are used? What kind of file structure is used?]**

Electronic files are saved in formats that comply with DCR's *File Format Guidelines for Management and Long-Term Retention of Electronic Records,* (http://www.records.ncdcr.gov/guides/file_formats_in-house_preservation_20120910.pdf). File formats used by the agency are adopted as standard by the state, and are well-supported, are backwards compatible, and have robust metadata support.

Maintained in a Secure Environment

Security to the system and to the records it holds is maintained in the following ways:

- Access rights are managed by the IT department, and are determined by a supervising authority to prevent unauthorized viewing of documents.
- The information technology system is able to separate confidential from nonconfidential information, or data creators organize and name file systems to reflect confidentiality of documents stored within
- Confidential information is stored on off-network storage systems, and folders with confidential information are restricted.
- Physical access to computers, disks, and external hard drives is restricted.
- Duplicate copies of digital media and system backup copies are stored in offsite facilities in order to be retrieved after a natural or human-made disaster.
- Confidential material is redacted **[define how]** before it is shared or otherwise made available.
- All system password and operating procedure manuals are kept in secure off-site storage (e.g. a bank safety deposit box).

Associated and Linked with Appropriate Metadata

Metadata is maintained alongside the record. At a minimum, metadata retained includes file creator, date created, title (stored as the file name), and when appropriate, cell formulae and email header information. Employees are not instructed to create metadata other than metadata that is essential for a file's current use and/or retention.

Stored on Media that is Regularly Assessed and Refreshed

Data is converted to new usable file types as old ones become obsolete or otherwise deteriorate. The following steps are taken to ensure the continued accessibility of records kept in electronic formats:

- Data is audited and assessed yearly
- Media is refreshed every three to five years. The agency documents when and how records are transferred from one storage medium to another.
- Records are periodically converted to new file types, particularly when a new information technology system requires that they be brought forward in order to properly render the file
- Metadata is maintained during migration
- Records are periodically verified through hash algorithms. This is done before and after migration to new media to ensure that the record did not change during conversion.
- Storage media is maintained in a manner and in an environment that promotes bit-level preservation. Humidity does not exceed 50% and should not fall below 30%. Room temperature is set between 65° F to 75° F. The agency adheres to the media manufacturer's recommendations for specific environmental conditions in which the media should be stored.
- Whatever media is used to store imaged data is clearly labeled with enough information that its contents can be determined.

5. Components of Information Technology System

[Describe how the agency ensures that its employees use the information system consistently and as intended. Describe what procedures are in place, what documentation is maintained, and what auditing controls are in place to ensure compliance and accuracy.]

- Training Programs
- Audit Trails
- Audits

Training Programs

The IT department will conduct training for system use and electronic records management, using material published by the Department of Cultural Resources when appropriate. All employees will be made aware of system procedures and policies, trained on them, and confirm by initialization or signature acknowledging that they are aware of the policies and have received training on them. When appropriate, employees will also attend trainings offered by the Department of Cultural Resources on the maintenance of electronic records. Documentation will be maintained for the distribution of written procedures, attendance of individuals at training sessions and refresher training programs and other relevant information.

Audit Trails

A log of activities on the system is maintained, which show who accessed the system, how and by whom records were created and modified, and whether standard procedures were followed.

Audits

Audits are designed to evaluate the process or system's accuracy, timeliness, adequacy of procedures, training provided, and the existence of audit trails. Internal audits are conducted regularly by agency IT staff.

6. Documentation of Information Technology System

[Describe what is contained within system documentation, who maintains it, and its retention period.]

- Content of System Documentation
- Retention of System Documentation

Content of System Documentation

The agency maintains system documentation that describes system procedures and actual practices, as well as system software and hardware, and the system environment in terms of the organizational structure, functions and responsibilities, and system processes. It explains how the system operates from a functional user and data processing point of view. Documentation is reviewed and updated **[yearly]** or upon implementation of a new information technology system by IT staff. Such documentation maintained by the agency includes:

- Procedural manuals
- System documentation
- Security backup and disaster recovery procedures as a part of the Continuity of Operations Plan
- System-level agreements for contracted information technology services

Retention of System Documentation

One set of all system documentation will be maintained during the period for which the records produced by the process or system could likely be subject to court review, and until all data created by every system instance has been destroyed or transferred to new operating environment. All such documentation is listed in the **[agency's, county, or municipal]** records retention schedule.

7. Digital Imaging Program Documentation and Procedures

[If your agency has or will be implementing an imaging program, describe the system in detail, including any hardware and software components; procedures for maintaining and operating the system; and how original and imaged records are managed.]

- System and Procedural Documentation
- Training
- Indexing and Metadata
- Auditing and Audit Trails
- Retention of Original and Duplicate Records

System and Procedural Documentation

[Document the information technology system used to produce and manage the agency's imaged records. This section should describe the system hardware and software, the system environment in terms of the organizational structure, functions and responsibilities, and the system processes. Documentation should be complete and up-to-date. If the agency outsources digital imaging, the service-level agreement should describe the operating environment and equipment. See Section 9 of this document, *Other Electronic Records Management Practices*, for more about contracting.]

[Example] The IT department is responsible for preparing and updating detailed procedures that describe the process followed to create and recreate electronic records. This documentation will include a description of the system hardware and software. A current procedural manual will be maintained to assure the most current steps are followed and to assure reliable system documentation will be available for judicial or similar proceedings.

Each workstation designated as a scanning station will have, at a minimum, the following hardware and software, unless the scanner is collocated by means of a network interface:

- Document/image scanner authorized by IT **[specify scanner manufacturer and model number]**
- Driver software for scanner
- Imaging software **[specify]**
- Instructions manual, maintained by IT staff, describing in detail the steps required to get from the beginning to the end of the process. This manual will also define:
    - The resolution of scanned images, as well as any compression standard used
    - The file formats of scanned images
    - The file naming conventions used for scanned images
    - If batch conversion or batch file re-naming will be necessary, and what tool is used for such conversions

  - How the scanned images will be stored in the file system
  - Any image enhancement techniques conducted after imaging

Training

[For agencies that scan in-house] Only designated staff that have been formally trained by IT staff and signed off on training documentation on the use of the imaging software and equipment will be allowed to enter records into the content management system. Covered records will be scanned and filed as part of an ongoing regularly conducted activity. Components of the training will include basic techniques for image capture, indexing, quality control, security configuration, auditing, use of equipment, and general system maintenance. Rights to image and index records will not be assigned until the user has been trained. If a user improperly indexes or scans a document, an auditor will address this occurrence with the operator and remedial training will be performed as necessary.

Indexing and Metadata

All imaged records must be indexed in order to facilitate efficient retrieval, ease of use, and up-to-date information about the images stored in the system. This index should capture the content, structure, and context of the imaged records, and will be developed by IT staff prior to the implementation of any imaging system. It should also be indexed according to guidelines set by the Department of Cultural Resources (see Section 9 of this policy, *Other Electronic Records Management Practices*, for more information on database indexing).

Auditing and Audit Trails

The imaging staff will conduct a quality control audit following the imaging of a record to ensure that the following features of the imaged record are legible:

- Individual letters, numbers, and symbols
- Combinations of letters, numbers, and symbols forming words or sentences
- Graphics such as signatures, logos, and pictures
- Other features of records such as color, shape, texture, etc., that relate to the content of the information

Managerial staff for the various units of the agency will also periodically audit imaged records for accuracy, readability, and reproduction capabilities. A written audit report will be prepared indicating the sampling of records produced and what remedial procedures were followed if the expected level of accuracy was not achieved.

Audit trails built into the imaging system will automatically document who creates, duplicates, modifies, or otherwise prepares records, and what procedures were taken. Audit trails include the success or failure, date, time, and user of the following events:

- Add/Edit electronic document
- Assign index template
- Copy document

- Copy pages
- Create document/folder
- Delete entry
- Delete pages
- Delete volume
- Edit image
- Email document
- Export document
- Index creation/deletion/modification
- Insert page
- Log in/out
- Move document
- Move pages
- Print document

Retention of Original and Duplicate Records

[For state agencies] The agency's records analyst at the Department of Cultural Resources will be contacted to amend the agency's records retention schedule to allow for the destruction of the original record following imaging.

[For local agencies] To obtain permission to destroy original records following imaging, this agency will complete Section 8 of this document, *Request for Disposal of Original Records Duplicated by Electronic Means*. For each new records series to be scanned, the Department of Cultural Resources must approve the destruction of the original records. Permanent records may be imaged for ease of access, but the original documents may not be destroyed unless an analog copy exists prior to the records' destruction.

[For state and local agencies] Destruction of original records is allowed only after quality assurance has been conducted on the imaged records, necessary corrections have been made, auditing procedures have been conducted, and the destruction is approved. Prior to destruction of the original record, managerial staff will audit a sample of those records to verify the accurate reproduction of those records.

Digital images of scanned records are maintained for the specified retention periods according to the records retention and disposition schedule. The retention period is considered to have begun when the original document was created, not when the electronic reproduction was created.

Electronic and digital images of scanned records in a document management system will be considered the "official" agency record. Any hard copy generated from the imaged records will be considered the agency's duplicate "working" record.

[For agencies that outsource scanning] A copy of the purchase order and a detailed service-level agreement with **[name of third-party organization]** is maintained. See Section 9 of this policy, *Other Electronic Records Management Practices,* for more information on contracting out electronic records management services.

8. Request for Disposal of Original Records Duplicated by Electronic Means

[For use by local agencies]

This form is used to request approval from the Department of Cultural Resources to dispose of non-permanent paper records which have been scanned, entered into databases, or otherwise duplicated through digital imaging or other conversion to a digital environment. This form does not apply to records which have been microfilmed or photocopied, or to records with a permanent retention.

[Insert the *Request for Disposal of Original Records Duplicated by Electronic Means* form into the policy here. The most up-to-date version of the form can be found on the State Archives website, www.ncdcr.gov/archives]

9. Other Electronic Records Management Practices

[Describe the agency's other electronic records management practices.]

- System Planning
- Electronic Records Management
- Database Indexing
- Security and Disaster Backup and Restoration
- **[For agencies that contract electronic records management services to third-party vendors]** Contracting

System Planning

[Explain for what purposes the agency uses traditional paper media, electronic systems, or microfilm, based on what format best serves the records retention requirements of unique records groups. Also explain how the agency plans for hardware and software updates, particularly how it takes future budgetary implications into consideration.]

Electronic Records Management

System documentation, system access records, digitization and scanning records, metadata, and information maintained by that system is listed in an approved records retention and disposition schedule prior to their destruction or other disposition.

[For state agencies] Records will be retained for the period of time required by agency records retention schedules and/or the General Schedule for State Agency Records regardless of format.

[For local agencies] Records produced by local agencies are retained for the period of time required by local records retention schedules regardless of format. Any permanent records maintained in electronic form also exist as a paper or microfilm preservation duplicate copy in compliance with the Department of Cultural Resources' *Human-Readable Preservation Duplicates* policy.

Database Indexing

G.S**.** §132-6.1 requires that databases be indexed with the Department of Cultural Resources. Indexes contain the following data fields:

- Description of the format or record layout
- Frequency with which the database is updated
- List of any data fields to which public access is restricted
- Description of each form in which the database can be copied or reproduced using the agency's computer facilities
- Schedule of fees for the production of copies in each available form

Security and Disaster Backup and Restoration

The agency has a disaster recovery plan for its electronic data in place, which includes contact information for data recovery vendors and information about back-ups of all data. Security back-ups to protect against data loss are generated for all but the most transitory of files. Routine back-ups are conducted **[define how often backups are conducted]**, and are stored in secure off-site storage **[define where back-ups are stored, and on what type of storage media]**.

[For agencies with imaging programs] Security backups of all imaged documents will be generated **[nightly]** and maintained off-site. Imaged documents will be synchronized to a secured offsite location **[immediately]** upon document changes or upon document scanning. A backup copy of the scanned data and index database is created **[on a nightly basis]** for the purpose of document recovery.

Cloud Computing

[For agencies that store electronic records cloud-based technology. Describe your agency's cloud-based practices. How is the technology used: as a storage site that mirrors locally hosted data, as the sole storage entity for data, or as a collaboration tool used during the drafting process? What backup measures? Should the vendor fail or should the agency otherwise discontinue service with the vendor, is the agency able to recover its electronic records, and in what form is that data available? For more guidance, please see the DCR guidance document, *Best Practices for Cloud Computing Records Management Considerations* at http://www.records.ncdcr.gov/guides/cloud_computing_final_20120801.pdf**]**

Contracting

[For agencies that contract out electronic records management services, including digital imaging]

The terms of the service level agreement with **[third-party contractor]** detail:

- How the vendor provides security, confidentiality, storage, and back-ups for electronic records.

- The equipment, including hardware and software, used by the vendor
- The storage environment, including any geographically disparate storage locations
- How the vendor complies with records retention requirements, including what the contractor is able to reproduce should legal proceedings or public records requests be issued
- How the vendor avoids spoliation of evidence once e-discovery has commenced
- How electronic records are to be recovered from the vendor in the event that the system is no longer supported

10. Compliance and Electronic Records Self-Warranty

[Depending on your agency's structure, this form may require the signatures of both the records custodian as well as Information Technology staff (or other project supervisor), as both have responsibility for the public records created by your units/sections/divisions. This form is structured to address the responsibilities of both entities.]

The completion of this form by all signing employees' signals that all employees of the unit/section/division will adhere to the rules set forth in this policy. Furthermore, this section is to be used as a self-evaluation tool to ensure that electronic records produced by state, county, municipal agencies, and other subdivisions of government are created, reproduced, and otherwise managed in accordance with guidelines for electronic public records published by the North Carolina Department of Cultural Resources. The self-warranting of records in itself does *not* authorize the destruction of records, originals or copies, *nor* does it change current records retention and disposition scheduling procedures.

The government agency producing electronic records and/or reproductions is responsible for ensuring the records' authenticity and accuracy. The Department of Cultural Resources is not responsible for certifying the authenticity or accuracy of any records, whether originals or reproductions, produced by the originating agency.

Records Custodian

The records custodian is the person responsible for creating records or managing the staff who creates records. The records custodian certifies that:

_______ The records created or duplicated by electronic means in this office are prepared in accordance with these guidelines as indicated by the following statements:

____

____

- Quality - Records are legible, accurate, and complete.
- The records are produced or reproduced as part of a regularly conducted activity.
- The records conform to DCR guidance regarding file formats, file naming, and if applicable digital preservation guidance produced by DCR.
- Detailed, documented procedures are in place and followed when the records are created, copied, modified, or duplicated.
- The person(s) who creates, copies, modifies, or duplicates the records receives formal training on detailed system procedures prior to records preparation.
- Details of the training received are adequately documented through written policies and procedures.
- Training records are signed by employee after receiving training.

_______ This agency will comply with the best practices and standards established by the Department of Cultural Resources as published on its website.

_______ **[Local Government Agencies]** This agency will submit to the Department of Cultural Resources Section 8 of this policy, *Request for Disposal of Original Records Duplicated by Electronic Means*, to seek approval for the destruction of original records that have been converted from paper to electronic record.

_______ **[State Government Agencies]** This agency will contact the Government Records Section to amend the agency schedule to comply with the best practices and standards established by the Department of Cultural Resources.

Approved by: ________________________________ Date: ____________________

Title: ________________________________

Signature: ________________________________

IT Professional or other Project Supervisor

The IT Professional is the person responsible for providing technical support to the records custodians and who may be involved in infrastructure and system maintenance. In the absence of an IT department, the supervisor of the records custodian should verify the following items. The IT Professional certifies that:

_______ Audit trails document the identity of the individual(s) who creates, duplicates, modifies, or otherwise prepares the records, what actions are taken by the individual during the course of the process, when these actions are taken, and what the results of these actions are.

_______ Audits:

- are performed periodically to confirm that the process or system produces accurate results.
- confirm that procedures actually followed are in accordance with procedure stated in the system's documentation.
- are performed routinely on documents to ensure no information has been lost.

____

- are performed by an independent source (i.e., persons other than those who create the records or persons without an interest in the content of the records. Acceptable source may include different department or authorized auditing authority).
- are adequately documented.

_______ The process or system hardware and software are adequately documented

_______ Permanent records conform to all file format, file naming, and digital preservation guidance produced by the Department of Cultural Resources.

_______ Back up procedures are in place and comply with best practices, as established by the Department of Cultural Resources.

_______ Successful disaster recovery back up is completed at least once every two years.

Approved by: ______________________________ Date: ____________________
Title: ______________________________

Signature: ______________________________

FOR DEPARTMENT OF CULTURAL RESOURCES USE

Approved by: ______________________________ Date: ____________________
Title: ______________________________

Signature: ______________________________